⇨Vendor: ISC

⇨Exam Code: SSCP

⇨Exam Name: System Security Certified Practitioner (SSCP)

New Updated Questions from Practicedump (Updated in Aug, 2022)

Visit Practicedump and Download Full Version SSCP Exam Dumps

**NEW QUESTION 220**
What kind of encryption is realized in the S/MIME-standard?
A. Elliptic curve based encryption
B. Asymmetric encryption scheme
C. Public key based, hybrid encryption scheme
D. Password based encryption scheme
**Answer: C**
Explanation:
Explanation/Reference:
S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and non-repudiation of electronic messages. S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages. The MIME standard therefore makes it possible to attach all types of files to e-mails. S/MIME was originally developed by the company RSA Data Security. Ratified in July 1999 by the IETF, S/ MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633.
How S/MIME works
The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.
The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.
The session key is inserted in each section's header, and is encrypted using the recipient's public key.
Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message.

In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.
Reference(s) used for this question:
http://en.kioskea.net/contents/139-cryptography-s-mime
RFC 2630: Cryptographic Message Syntax;
OPPLIGER, Rolf, Secure Messaging with PGP and S/MIME, 2000, Artech House; HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 570; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

**NEW QUESTION 221**
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?
A. Intrusion Detection System
B. Intrusion Management System (IMS)
C. Compliance Validation System
D. Compliance Monitoring System
**Answer: A**
Explanation:
Section: Analysis and Monitoring
Explanation/Reference:
An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's system security policy have taken place.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

**NEW QUESTION 222**
What is the main characteristic of a multi-homed host?
A. It has multiple network interfaces, each connected to separate networks.
B. It is placed between two routers or firewalls.
C. It operates at multiple layers.
D. It allows IP routing.
**Answer: A**
Explanation:
Section: Network and Telecommunications
Explanation/Reference:
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.
Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

**NEW QUESTION 223**
Encapsulating Security Payload (ESP) provides some of the services of Authentication Headers (AH), but it is

primarily designed to provide:
A. Digital signatures
B. Access Control
C. Confidentiality
D. Cryptography
**Answer: C**
Explanation:
Explanation/Reference:
Source: TIPTON, Harold F & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 164.

**NEW QUESTION 224**
A public key algorithm that does both encryption and digital signature is which of the following?
A. RSA
B. IDEA
C. Diffie-Hellman
D. DES
**Answer: A**
Explanation:
Explanation/Reference:
RSA can be used for encryption, key exchange, and digital signatures.
Key Exchange versus key Agreement
KEY EXCHANGE
Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.
If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require depends on the encryption technique they might use. If they use a code, both will require a copy of the same codebook. If they use a cipher, they will need appropriate keys. If the cipher is a symmetric key cipher, both will need a copy of the same key. If an asymmetric key cipher with the public/private key property, both will need the other's public key.
KEY AGREEMENT
Diffie-Hellman is a key agreement algorithm used by two parties to agree on a shared secret. The Diffie Hellman (DH) key agreement algorithm describes a means for two parties to agree upon a shared secret over a public network in such a way that the secret will be unavailable to eavesdroppers. The DH algorithm converts the shared secret into an arbitrary amount of keying material. The resulting keying material is used as a symmetric encryption key.
The other answers are not correct because:
DES and IDEA are both symmetric algorithms.
Diffie-Hellman is a common asymmetric algorithm, but is used only for key agreement. It is not typically used for data encryption and does not have digital signature capability.
References:
http://tools.ietf.org/html/rfc2631
For Diffie-Hellman information: http://www.netip.com/articles/keith/diffie-helman.htm

**NEW QUESTION 225**

Which access control model would a lattice-based access control model be an example of?
A. Discretionary access control.
B. Rule-based access control.
C. Non-discretionary access control.
D. Mandatory access control.
**Answer: D**
Explanation:
Explanation/Reference:
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.
TIPS FROM CLEMENT
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.
Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:
FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.
SECOND: DAC (Discretionary Access Control)
Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.
THIRD: MAC (Mandatory Access Control)
All of the following are forms of Mandatory Access Control:
Mandatory Access control (MAC) (Implemented using the lattice)
You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.
All of the following are forms of Non Discretionary Access Control:
Role Based Access Control (RBAC)
Rule Based Access Control (Think Firewall in this case)
The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.
I hope this clarifies the whole drama related to what is what in the world of access control.
In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).
The following answers are incorrect:

Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.
Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.
Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.
References:
AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

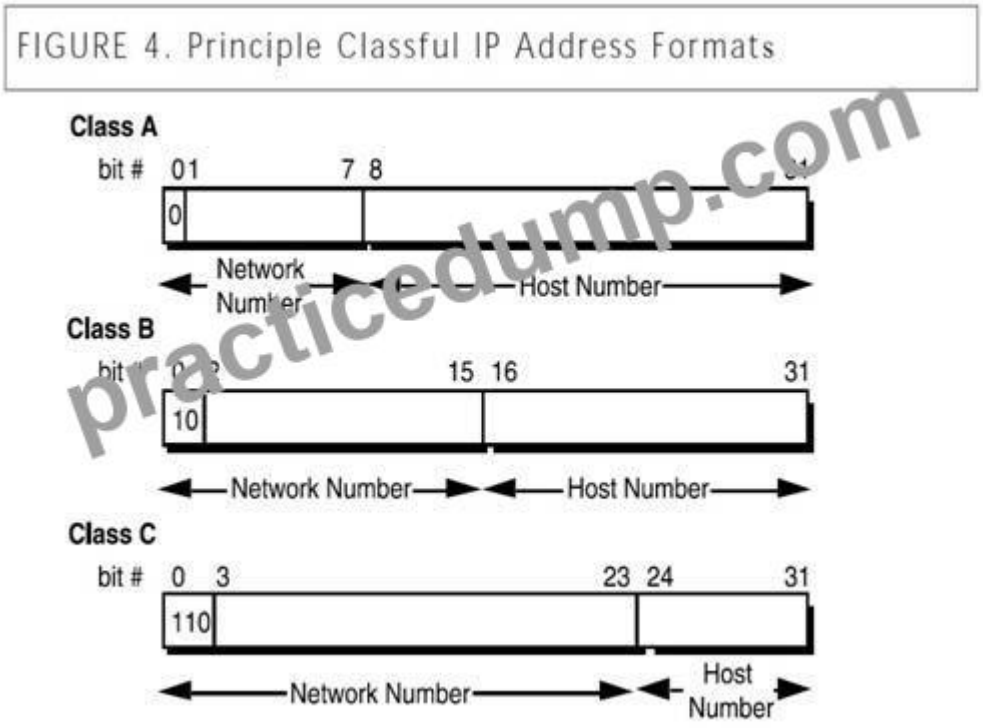
**NEW QUESTION 226**
What is RAD?
A. Risk-assessment diagramming
B. A development methodology
C. A project management technique
D. A measure of system complexity
**Answer: B**
Explanation:
Explanation/Reference:
RAD stands for Rapid Application Development.
RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.
RAD is a programming system that enables programmers to quickly build working programs.
In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.
Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.
Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.
Reference:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)
http://www.webopedia.com

**NEW QUESTION 227**
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

A. Screened subnets
B. Digital certificates
C. An encrypted Virtual Private Network
D. Encryption
**Answer: C**
Explanation:
Virtual Private Networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet.
Screened Subnet: A screened subnet is essentially the same as the screened host architecture, but adds an extra strata of security by creating a network which the bastion host resides (often call perimeter network) which is separated from the internal network. A screened subnet will be deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.
Digital Certificates: Digital Certificates will be used in the intitial steps of establishing a VPN but they would not provide the encryption and integrity by themselves.
Encryption: Even thou this seems like a choice that would include the other choices,
encryption by itself does not provide integrity mechanims. So encryption would satisfy only
half of the requirements of the question.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 65).

**NEW QUESTION 228**
In the days before CIDR (Classless Internet Domain Routing), networks were commonly organized by classes. Which of the following would have been true of a Class B network?
A. The first two bits of the IP address would be set to one, and the third bit set to zero.
B. The first bit of the IP address would be set to zero.
C. The first three bits of the IP address would be set to one.
D. The first bit of the IP address would be set to one and the second bit set to zero.
**Answer: A**
Explanation:
Explanation/Reference:
Each Class B network address has a 16-bit network prefix, with the two highest order bits set to 1-0.
The following answers are incorrect:
The first bit of the IP address would be set to zero. Is incorrect because, this would be a Class A network address.
The first two bits of the IP address would be set to one, and the third bit set to zero. Is incorrect because, this would be a Class C network address.
The first three bits of the IP address would be set to one. Is incorrect because, this is a distractor. Class D & E have the first three bits set to 1. Class D the 4th bit is 0 and for Class E the 4th bit to 1.
Classless Internet Domain Routing (CIDR)
High Order bits are shown in bold below.
For Class A, the addresses are 0.0.0.0 - 127.255.255.255
The lowest Class A address is represented in binary as 00000000.00000000.0000000.00000000 For Class B networks, the addresses are 128.0.0.0 - 191.255.255.255.
The lowest Class B address is represented in binary as 10000000.00000000.00000000.00000000 For Class C,

the addresses are 192.0.0.0 - 223.255.255.255
The lowest Class C address is represented in binary as 11000000.00000000.00000000.00000000 For Class D, the addresses are 224.0.0.0 - 239.255.255.255 (Multicast)
The lowest Class D address is represented in binary as 11100000.00000000.00000000.00000000 For Class E, the addresses are 240.0.0.0 - 255.255.255.255 (Reserved for future usage) The lowest Class E address is represented in binary as 11110000.00000000.00000000.00000000 Classful IP Address Format






References:
3Com http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf
AIOv3 Telecommunications and Networking Security (page 438)

**NEW QUESTION 229**
Address Resolution Protocol (ARP) interrogates the network by sending out a?
A. unicast.
B. multicast.
C. broadcast.
D. semicast.
**Answer: C**
Explanation:
ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. A broadcast message is sent to everyone whether or not the message was requested. A traditional unicast is a "one-to-one" or "narrowcast" message. A multicast is a "one-tomany" message that is traditionally only sent to those machine that requested the information. Semicast is an imposter answer. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

**NEW QUESTION 230**

What type of attack involves IP spoofing, ICMP ECHO and a bounce site?
A. SYN attack
B. Teardrop attack
C. IP spoofing attack
D. Smurf attack
**Answer: D**
Explanation:
A smurf attack occurs when an attacker sends a spoofed (IP spoofing) PING (ICMP ECHO) packet to the broadcast address of a large network (the bounce site). The modified packet containing the address of the target system, all devices on its local network respond with a ICMP REPLY to the target system, which is then saturated with those replies. An IP spoofing attack is used to convince a system that it is communication with a known entity that gives an intruder access. It involves modifying the source address of a packet for a trusted source's address. A teardrop attack consists of modifying the length and fragmentation offset fields in sequential IP packets so the target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets. A SYN attack is when an attacker floods a system with connection requests but does not respond when the target system replies to those requests. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 76).

**NEW QUESTION 231**
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?
A. Recreating and analyzing the problem
B. Estimating the cost of the changes requested
C. Establishing the priorities of requests
D. Determining the interface that is presented to the user
**Answer: C**
Explanation:
Section: Security Operation Adimnistration
Explanation/Reference:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

**NEW QUESTION 232**
Which of the following algorithms is used today for encryption in PGP?
A. Blowfish
B. IDEA
C. RSA
D. RC5
**Answer: B**
Explanation:
Section: Cryptography
Explanation/Reference:

The Pretty Good Privacy (PGP) email encryption system was developed by Phil Zimmerman. For encrypting messages, it actually uses AES with up to 256-bit keys, CAST, TripleDES, IDEA and Twofish. RSA is also used in PGP, but only for symmetric key exchange and for digital signatures, but not for encryption.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (pages 154, 169).
More info on PGP can be found on their site at http://www.pgp.com/display.php?pageID=29.

**NEW QUESTION 233**
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:
A. you need.
B. you read.
C. you do.
D. you are.
**Answer: D**
Explanation:
Section: Access Control
Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

**NEW QUESTION 234**
Corporate networks are safer if an end user connects through a VPN connection?
A. True
B. False
**Answer: B**

**NEW QUESTION 235**
.....